

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Previously Presented) A file security system for restricting access to electronic files, said file security system comprising:

a key store configured to store a plurality of cryptographic key pairs, wherein the cryptographic key pairs include a respective public key and a respective private key, at least one of the cryptographic key pairs pertaining to a predetermined time, being uniquely generated each day; and

an access manager, configured to operatively connect to said key store, configured to determine whether the private key of at least one of the cryptographic key pairs pertaining to the predetermined time is permitted to be provided to a requestor based on a current time,

wherein the access manager is configured to require that the requestor use the private key pertaining to the predetermined time to access a document key in an encrypted header of a secured electronic file, a data portion of the secured electronic file which was previously secured using the document key, and wherein the header includes the document key and access rules for the secured electronic file, the access rules configured to further protect the document key and provide

restrictive access to the data portion, and wherein the header comprising the document key and the access rules was previously encrypted by the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time.

2. (Previously Presented) The file security system as recited in claim 1, wherein said access manager is configured to provide the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to the requestor in response to determining that the predetermined time is earlier than or equal to the current time.

3. (Previously Presented) The file security system as recited in claim 1, wherein the requestor is a client module that is configured to operatively connect to said access manager over a network.

4. (Previously Presented) The file security system as recited in claim 1, wherein said file security system further comprises:

at least one client module configured to select the predetermined time and to secure the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time, so as to provide a time-based access restriction to the electronic file.

5. (Previously Presented) The file security system as recited in claim 4, wherein said client module is further configured to unsecure the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time from said key store, and then unsecure the secured electronic file using the private key pertaining to the predetermined time.

6. (Previously Presented) A method for restricting access to an electronic document, said method comprising:

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data, and a header portion that contains access rules for the electronic document, the access rules providing restrictive access to the data portion;

securing the data portion of the electronic document through use of a document key to produce a secured electronic document;

storing the document key in the header portion of the electronic document, wherein the access rules are provided for further protecting the document key;

securing the header portion of the electronic document, comprising the document key and the access rules, through the use of a time-based access key, being uniquely generated each day; and

storing the secured electronic document.

7. (Previously Presented) The method as recited in claim 6, wherein securing the header portion comprises securing the header portion with a time-based access key that has an access time associated therewith.

8. (Previously Presented) The method as recited in claim 7, further comprising:

storing the time-based access key at a remote key store, wherein the time-based access key is subsequently retrievable from the remote key store when the current time is equal to or later than the access time associated with the time-based access key.

9. (Previously Presented) The method as recited in claim 8, wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network.

10. (Previously Presented) A method for restricting access to an electronic document, said method comprising:

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data, and a header portion that contains access rules for the electronic document, the access rules providing restrictive access to the data portion;

obtaining a document key;

encrypting the data portion of the electronic document using the document key to produce an encrypted data portion;

obtaining a time-based access key, being uniquely generated each day;

encrypting the document key in conjunction with the access rules using the time-based access key to produce an encrypted document key;

storing the encrypted document key in the header portion;

protecting the document key using the access rules;

forming a secured electronic document from at least the encrypted data portion and the header; and
storing the secured electronic document.

11. (Previously Presented) The method as recited in claim 10, wherein encrypting the document key comprises encrypting the document key using a public time-based access key.

12. (Previously Presented) The method as recited in claim 10, wherein encrypting the document key comprises encrypting the document key using a time-based access key that has an access time associated therewith.

13. (Previously Presented) The method as recited in claim 12, wherein obtaining a time-based access key comprises obtaining a time-based access key that is available from a remote key store when the current time is equal to or later than the access time associated with the time-based access key.

14. (Previously Presented) The method as recited in claim 13, wherein obtaining a time-based access key comprises obtaining a time-based access key that specifies an access time as a specified day of a year, and
further comprising obtaining a different unique time-based access key for a plurality of different days of the year.

15. (Previously Presented) The method as recited in claim 13, wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network.

16. (Previously Presented) A method for providing a secured electronic document to a requestor, the secured electronic document having at least a header portion, having a document key encrypted in conjunction with access rules, and an encrypted data portion, said method comprising:

obtaining a time-based access key, being uniquely generated each day;

decrypting the document key and the access rules using the time-based access key, access to the document key being subject to protection by the access rules;

decrypting the encrypted data portion of the secured electronic document using the document key to produce a non-encrypted data portion, the access rules providing restrictive access to the data portion; and

supplying the non-encrypted data portion to the requestor.

17. (Previously Presented) The method as recited in claim 16, wherein obtaining a time-based access key comprises obtaining a time-based access key that is identified by an indicator within a header portion of the secured electronic document.

18. (Previously Presented) The method as recited in claim 16, wherein obtaining a time-based access key comprises obtaining a private time-based access key.

19. (Previously Presented) The method as recited in claim 18, wherein obtaining a time-based access key comprises acquiring the time-based access key from a server.

20. (Previously Presented) The method as recited in claim 16, wherein said obtaining of the time-based access key is dependent on a current time.

21. (Previously Presented) The method as recited in claim 16, wherein obtaining a time-based access key comprises obtaining a time-based access key that is associated with an access time, and wherein said obtaining of the time-based access key is permitted at a current time when the current time is later than or equal to the access time.

22. (Previously Presented) The method as recited in claim 21, wherein obtaining a time-based access key comprises obtaining the time-based access key from a server.

23-25. (Cancelled)

26. (Previously Presented) A non-transitory tangible computer-readable medium having instructions stored thereon, the instructions comprising:

computer program code configured to identify an electronic document to be secured, the electronic document having at least a data portion that contains data, and a

header portion that contains access rules for the electronic document, the access rules providing restrictive access to the data portion;

computer program code configured to secure the data portion of the electronic document through use of a document key to produce a secured electronic document;

computer program code configured to store the document key in the header portion of the electronic document;

computer program code configured to protect the document key using the access rules;

computer program code configured to secure the header portion of the electronic document, comprising the document key and the access rules, through the use of a time-based access key, being uniquely generated each day; and

computer program code configured to store the secured electronic document.

27. (Previously Presented) The computer readable medium as recited in claim 26, wherein the time-based access key is configured to have an access time associated therewith.

28. (Previously Presented) The computer readable medium as recited in claim 27, wherein said computer readable medium further comprises:

computer program code configured to store the time-based access key at a remote key store, and

computer program code configured to retrieve the time-based access key from the remote key store at a current time that is later than or equal to the access time associated with the time-based access key.

29. (Previously Presented) A non-transitory tangible computer-readable medium having stored thereon computer-executable instructions that, in response to execution by a computing device, cause the computing device to perform a method comprising:

identifying an electronic document to be secured, the electronic document having at least a data portion that contains data, and a header portion that contains access rules for the electronic document, the access rules providing restrictive access to the data portion;

securing the data portion of the electronic document through use of a document key to produce a secured electronic document;

storing the document key in the header portion of the electronic document;

protecting the document key using the access rules;

securing the header portion of the electronic document, comprising the document key and the access rules, through the use of a time-based access key, being uniquely generated each day; and

storing the secured electronic document.

30. (Previously Presented) A non-transitory tangible computer-readable medium having stored thereon computer-executable instructions that, in response to

execution by a computing device, cause the computing device to perform a method comprising:

identify an electronic document to be secured, the electronic document having at least a data portion that contains data, and a header portion that contains access rules for the electronic document, the access rules providing restrictive access to the data portion;

obtain a document key;

encrypt the data portion of the electronic document using the document key to produce an encrypted data portion;

obtain a time-based access key, being uniquely generated each day;

encrypt the document key in conjunction with the access rules using the time-based access key to produce an encrypted document key;

store the encrypted document key in the header portion;

protect the document key using the access rules;

form a secured electronic document from at least the encrypted data portion and the encrypted header; and

store the secured electronic document.

31. (Previously Presented) A non-transitory tangible computer-readable medium having stored thereon computer-executable instructions that, in response to execution by a computing device, cause the computing device to perform a method comprising:

obtain a time-based access key, being uniquely generated each day;

decrypt a document key and access rules in a header portion using the time-based access key, access to the document key subject to protection by access rules in the header portion;

decrypt an encrypted data portion of the secured electronic document using the document key to produce a data portion, the access rules providing restrictive access to the data portion; and

supply the data portion to the requestor.

32. (Previously Presented) The method of claim 6, further comprising:

determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based access key for the predetermined time.

33. (Previously Presented) The computer-readable medium of claim 26, further comprising:

computer program code configured to determine whether a time-based access key is already available for a predetermined time, otherwise generating a time-based access key for the predetermined time.

34. (Previously Presented) The computer-readable medium of claim 29, further comprising:

Reply to Office Action of December 13, 2011

Nicholas M. RYAN
Appl. No. 10/676,850

determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based access key for the predetermined time.